CLAIMS:

1. In a Mobile IP visiting domain, a route optimization technique requiring no awareness of the Mobile IP protocol by a Correspondent Node when forwarding datagrams using the shortest path between the Mobile Node and the Correspondent Node.

2. The route optimization technique of claim 1, wherein a Mobile IP Foreign Agent adds an entry in its routing table when the Mobile Node registers in a visiting domain.

3. The route optimization technique of claim 2, wherein the Foreign Agent removes the route entry when the Mobile Node de-registers or the registration times out.

4. The route entry of claim 3, wherein the Mobile Node home network address is the destination, the local interface to which the Mobile Node is attached is the nexthop and the cost for the route is set lower than any other route available to the Mobile Node (including the route pointing to the Home Agent tunnel).

5. The route entry of claim 4, wherein routing based on the destination address is performed.

6. The route entry of claim 5, wherein the route propagation is limited by a route policy to be spread in an OSPF area, a BGP autonomous system or not at all.

7. The route entry of claim 3, wherein the source address is the Mobile Node, the destination address is a selected set of subnetworks in the Foreign Agents vicinity, and the nexthop is a local interface of the Foreign Agent.

8. The route entry of claim 7, wherein source-restricted destination address routing is performed.

9. The route entry of claim 8, wherein the route is not propagated to other routers using a routing protocol.

10. The route optimization technique of claim 1, wherein a dynamic Network Address Translation is performed in the Foreign Agent for traffic sent from the Mobile Node to Corresponding Nodes in the visiting domain.

11. The Network Address Translation of claim 10, wherein the state table is indexed by Mobile Node home network address (private) and a unique link layer address (e.g. MAC).

12. The state table of claim 11, wherein the state is accepted as long as the Mobile Node has a valid registration with the Home Agent as determined by active Foreign Agent state in the Mobile IP process for unique link layer address (e.g. MAC).

13. The state table of claim 11, wherein the state is denied if the Mobile Node does not have a valid registration with the Home Agent.

14. The state table of claim 11, wherein the state, in order to be unique, is indexed by link layer type with which the Mobile Node attaches to the Foreign Agent.

15. The route optimization technique of claim 1, wherein static routes and filtering rules for the Mobile Node is distributed to the Foreign Agent.

16. The filter rules of claim 15, wherein static routes and filters are distributed to the Foreign Agent at configuration time.

17. The filter rules of claim 15, wherein static routes and filters are distributed to the Foreign Agent as part of the mobile IP registration.

18. The filter distribution of claim 17, wherein static routes and filters are piggybacked in a DIAMETER response from the home agent to the foreign agent.

19. The filter rules of claim 15, wherein the filters are tied to the Mobile Node home network address and Home Agent address.

20. The filter installation of claim 19, wherein the filters are applied to Mobile Node traffic sent out on the local subnet as long as a valid Mobile IP registration exists with the Home Agent.

21. The filter installation of claim 20, wherein the filters are blocked for Mobile Node traffic if no valid Mobile IP registration exists with the Home Agent.

22. The route optimization technique of claim 1, wherein a care-of address is allocated to the Mobile Node using dynamic host configuration, when entering a visited network and no separate Foreign Agent is found.

23. The co-located care-of address of claim 22, wherein the care-of address is applied as source address to a virtual interface adapter in the Mobile Node to be used for local traffic towards destination on the visited network optionally limited by port number.

24. The virtual interface adapter of claim 23, wherein virtual interface adapter is enabled at Mobile IP registration.

25. The virtual interface adapter of claim 24, wherein virtual interface adapter is disabled when the Mobile IP registration is no longer valid or moves from the visited subnetwork to a new subnetwork.

26. The virtual interface adaptor of claim 25, wherein the Home Agent tunnel is given a lower cost as nexthop compared to local IP connectivity for static routes received as part of the mobile IP registration procedure with the Home Agent.

27. The selective reverse tunneling technique of claim 26, wherein the mobile IP registration procedure involves a dynamic host configuration procedure in the home domain.

28. The dynamic host configuration of claim 27, wherein the static routes retrieved during the dynamic host configuration procedure are piggy-backed as an extension in the Mobile IP registration reply message.

29. The virtual interface adaptor of claim 25, wherein local IP connectivity is given lower cost as nexthop compared to Home Agent tunnel for static routes received as part of the dynamic host configuration protocol procedure in the visited domain.

30. The co-located care-of address of claim 22, wherein the Mobile Node applies filter rules for traffic being sent and received with local IP connectivity and Home Agent tunnel respectively.

31. The filter rules of claim 30, wherein filter rules are loaded into the Mobile Node at configuration time.

32. The filter rules of claim 30, wherein the filter rules are loaded as part of the Mobile IP registration procedure with the Home Agent when entering the visiting domain.

33. The filter distribution of claim 32, wherein the filter rules are piggybacked to the Mobile IP registration reply message as an extension.

34. The route optimization technique of claim 1, wherein the selective reverse tunneling is applied between Home Agent tunnel and local IP connectivity using route prefix and cost.

35. The selective reverse tunneling technique of claim 34, wherein the Home Agent tunnel route is given a lower cost as nexthop compared to local IP connectivity in case of overlapping private address realms for visited and home network.

36. The selective reverse tunneling technique of claim 34, wherein the Home Agent tunnel route is given a lower cost as nexthop compared to local IP connectivity in case of Internet access.

37. The selective reverse tunneling technique of claim 34, wherein local IP connectivity is given lower cost as nexthop compared to the Home Agent tunnel for routes belonging to the same subnetwork as the Mobile Node.

38. The selective reverse tunneling technique of claim 34, wherein the Home Agent tunnel is given a lower cost as nexthop compared to local IP connectivity for routes belonging to the home network.

39. The route optimization technique of claim 1, wherein multiple Home Agents are hosting the home network using the same IP address to which a Mobile Node can send registration requests and datagrams all with the same UDP port number.

40. The multi-homed home network of claim 39, wherein a Load Balancer is dispatching the registration requests and corresponding UDP tunneled datagrams across the Home Agents using the layer 2 bridge-path method based on IP source address and UDP source port number.

41. The multi-homed home network of claim 40, wherein a Home Agent retrieves the mobile user data from a common AAA server or LDAP directory at Mobile IP registration time.

42. The multi-homed home network of claim 41, wherein the selected Home Agent sends registration reply and UDP tunneled datagrams to the care-of address using the direct server return method.

43. The multi-homed home network of claim 42, wherein the Home Agent uses a unique IP address (different from the Home Agent IP address) in sending routing updates to other routers related to the Mobile Node availability.

44. The route optimization technique of claim 1, wherein a Load Balancer or other router along the path sends an ICMP (Type 3) Destination Unreachable message to the tunnel decapsulator (Mobile Node or Foreign Agent) in case of failure of the Home Agent that is the assigned to serve the UDP port number used by the Mobile Node or Foreign Agent. Further comprising, that this tunnel soft state is reported to the originator (Mobile Node) as (Type 3 Code 0) Network Unreachable in the case the Foreign Agent is the decapsulator.

45. The redundancy technique of claim 44, wherein the Mobile Node sends a new registration towards the same Home Agent IP address after receiving the ICMP destination unreachable message.

46. The redundancy technique of claim 45, wherein the Load Balancer performs a heart beat control that a Home Agent is alive before allocating a registration request to the Home Agent.

47. The redundancy technique of claim 46, wherein the Load balancer allocates a new Home Agent for the Mobile Node when receiving the new registration request.

48. The redundancy technique of claim 45, wherein one Home Agent acts as primary and another Home Agent as secondary for a Home Agent IP address:
Having the primary Home Agent send a virtual router redundancy protocol packet with type other than 1 to relay Mobile Node registration requests; and
Having the secondary node overtake the Home Agent IP address of the primary node in case of detecting failure to the first node using the virtual router redundancy protocol (VRRP) packet type equal 1.

49. The route optimization technique of claim 1, wherein the care-of address may reside behind a network address translation and the Home Agent will reject the first registration request from the Mobile Node, by including a new challenge, if the IP source address header of the registration request is different from the care-of address field in the registration request.

50. The network address translation traversal of claim 49, wherein the Mobile Node will send a response to the challenge as part of the second registration request with which the Home Agent can validate the identity of the source of the registration request.

51. The network address translation traversal of claim 50, wherein the Home Agent uses the IP source address header of the registration request as the destination address for datagram encapsulation towards the care-of address.

52. The network address translation traversal of claim 51, wherein the node carrying the care-of address (Mobile Node or Foreign Agent) will use the IP source address header of the registration reply as the source address for datagram encapsulation towards the Home Agent.

53. The network address translation traversal of claim 49, wherein address masquerading is performed using a port translation and the payload datagrams are tunneled from the care-of address to the Home Agent using User Datagram Protocol (UDP) between the inner and outer IP header and IP header compression (RFC 2507) on the outer UDP/IP header.

54. The route optimization technique of claim 1, wherein Mobile IP security associations between the Mobile Node, Home Agent and Foreign Agent are established using X.509 public key certificates with a Common Name or Subject Alternative Name equaling the UFQDN (User Fully Qualified Domain Name) or home network address of the Mobile Node, and the certificate being signed by the Mobile Service Manager certificate authority.

55. The mobile IP public key security associations of claim 54, wherein the Foreign Agent and Home Agent are configured with its own and its Mobile Service Manager's certificate, and the Mobile Node is configured with its own, its Mobile Service Manager's and its Home Agent's certificate.

56. The mobile IP public key security associations of claim 55, wherein the Mobile Node and the Foreign Agent include their certificates as a Mobile IP extension in the registration request message and the Home Agent includes its and the Foreign Agent's certificate as a Mobile IP extension in the registration reply message.

57. The mobile IP public key security associations of claim 56, wherein the party receiving a certificate is verifying the signature of using the certificate of the Mobile Service Manager.

58. The mobile IP public key security associations of claim 57, wherein the party receiving a certificate is matching it with the certificate revocation list given by the Mobile Service Manager at configuration time, through an online certificate status protocol RFC 2560, or a DNS Security RFC 2535 request.

59. The mobile IP public key security associations of claim 58, wherein the Home Agent validates the Foreign Agent's certificate on behalf of the Mobile Node and sends a signed Foreign Agent certificate to the Mobile Node in the registration reply message.

60. The mobile IP public key security associations of claim 58, wherein the party receiving a certificate is applying the public key of the certificate to the authenticator in the Mobile IP Authentication Extension if the policy specifies that certificates with Mobile Service Manager signature shall be trusted, signature verification is successful and no matching record was found in the revocation list.

61. The mobile IP public key security associations of claim 60, wherein the Mobile Node is applying the public key of Foreign Agent certificate to the authenticator in the Mobile IP Authentication Extension if the policy specifies that certificates with Home Agent signature shall be trusted and signature verification is successful.

62. The mobile IP public key security associations of claim 60, wherein the receiving party establishes a Security Parameter Index (SPI) equal to a

predetermined 4-byte integer larger than 255 (denoting X.509 certificate usage) between the pair of nodes in case the authentication is successful.

63. The mobile IP public key security association of claim 62, wherein the Mobile Node, Foreign Agent and Home Agent may use the same X.509 certificate in order to establish IP security or transport layer security among each other.

~~62~~ 64. The mobile IP public key security association of claim 61, wherein the Foreign Agent and Home Agent act as network or transport layer security proxies for a Mobile Node accessing the servers in the home network and visited network respectively.